Managing Your Passwords Now and Forever

Gail Weiss

Agenda – Managing Passwords

- Using Different Passwords for Every Site
- Tips for Strong Passwords
- Two Factor Authentication
- Password Manager Applications
- Google Chrome – Managing Passwords on your Computer and iPhone

Agenda – Digital Legacy

- What Not to Do
- Deleting Accounts After Death
- Computer & Laptops Guide
- Mobile Phone Guide
- Accessing your iPhone Assets
- Facebook – Deleting Account After Death
- Google – Inactive Account Mgr
- Photos, Music & Other Files
- Financial Accounts & Utilities
- Password Lists
- Sample of Digital Legacy Template
- Links to More Info

Managing Passwords

Using Different Passwords for Every Site

- One Single Strong Password Isn't Enough Anymore
- Use of Different Strong Password for Every Important On-Line Account
- Devise a Way to Manage Them All

Using Different Passwords for Every Site

- If you use a Single Password everywhere, a single leak of that password puts all your other accounts at risk
- Hacker breaches Service A's security –
  - Gets your Login ID, Password and Security Questions
  - Now has access to Service B, C & etc.
- Phishing Email Messages Asking for Password
- Improper Use of Open Wi-Fi Hotspot

Tips for Strong Passwords

- Eight to Twelve Characters Minimally
- One Uppercase Letter, Numbers and Special Characters
- Randomly Generated (i.e. By LastPass and other Password Manager Programs)

Two Factor Authentication

- Cybersecurity threats are multiplying with each passing year. They are growing more sophisticated, as shown by the continued success enjoyed by ransomware and other scams. Two-factor authentication is a time-tested way to minimize the threat of a breach and protect the organization as well as the individual from attacks.

Types of 2FA

- TYPES OF 2FA
- Secondary authentication factors vary in how they are used in the verification of user identities. Options range from passcodes to biometrics and codes, with the latter being by far the most common 2FA method, typically via a text message.
- The simple expedient of texting a time-sensitive code to a mobile device is usually enough to keep most accounts secure. This approach offers benefits that make it more acceptable to users, such as simplicity and speed of access. But it does require users to register a mobile number. If that device gets lost, stolen or damaged, the user won't be able to validate their own identity and access their data and applications. Further, some users are sensitive to the privacy liabilities of handing their mobile number to a third party.
- **Don't use your land line for 2FA**

Password Managers

- **Are password managers safe to use? Find out if they are really secure and discover the benefits and risks of using password managers.**
- Yes. Password managers are a safer way to manage and secure passwords than any other approach. They may not be perfect, but what are the alternatives — posting notes on computer screens, keeping a file of passwords saved on your desktop, using the same two or three passwords over and over with variations, or sticking to default passwords like “admin” or “1234”?
- Hackers love those who use these methods, as they are easier to crack than the complex and random passwords generated by password managers.
- That isn’t to say that password managers don’t have frailties. Once you know the master password, you can access all associated accounts. But adherence to best practices such as adding two-factor authentication can minimize those risks.

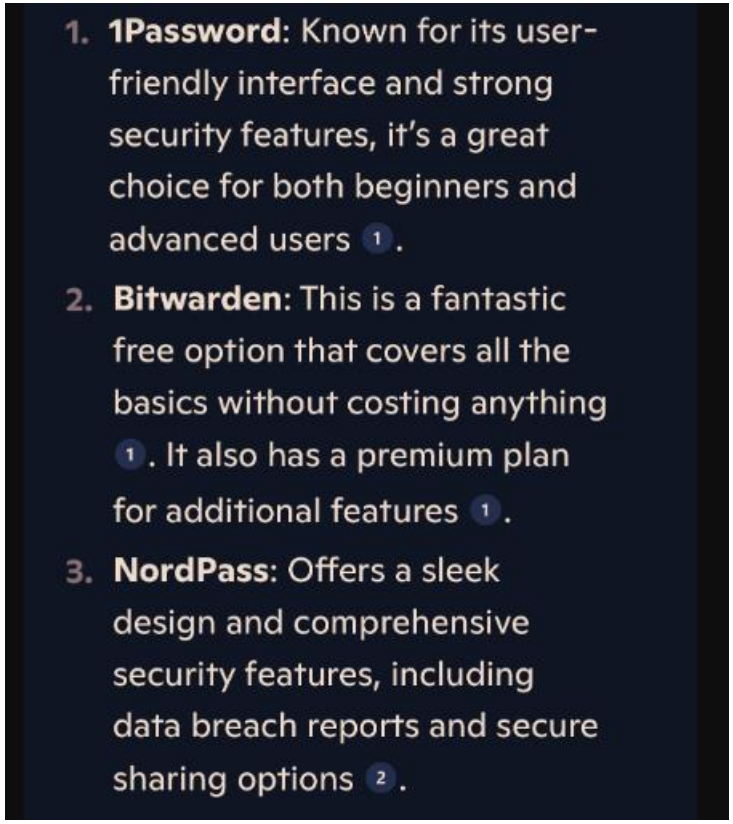
Password Managers

- **How do password managers work?**
- A password manager is basically an app or vault that stores your passwords, so there is no need to remember them. The user simply logs into the password manager using a master password. Once unlocked, the password manager app uses the passwords stored in its encrypted vault to access all other user accounts. For account setups or first-time logins, the password manager generates long and complex passwords for each site or application and enters them into websites and apps automatically.
- Those using password managers are advised to turn on and always use two-factor authentication. With that on, a criminal who knows the master password won't be able to access user data and logins as they can't provide the code or biometric input called for in 2FA. Additionally, password manager users should create a strong password as the master — one they can easily remember but is long enough and has a variation of upper and lowercase letters, symbols, and numbers to thwart hackers.

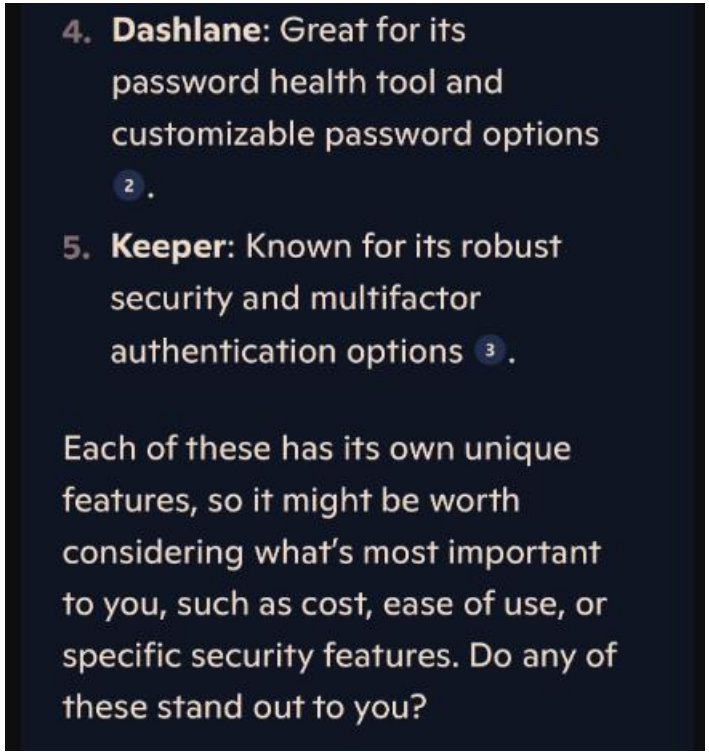
Password Managers

- Once you purchase a password manager, it needs to be downloaded onto your computer and/or mobile device. You're walked through the stages of setting a master password, activating 2FA and choosing the best authentication method, adding password extensions to browsers, and logging in to your various accounts to change existing passwords. The changed passwords are generated by the password manager, encrypted, and stored in its secure vault.

AI recommending Password Managers



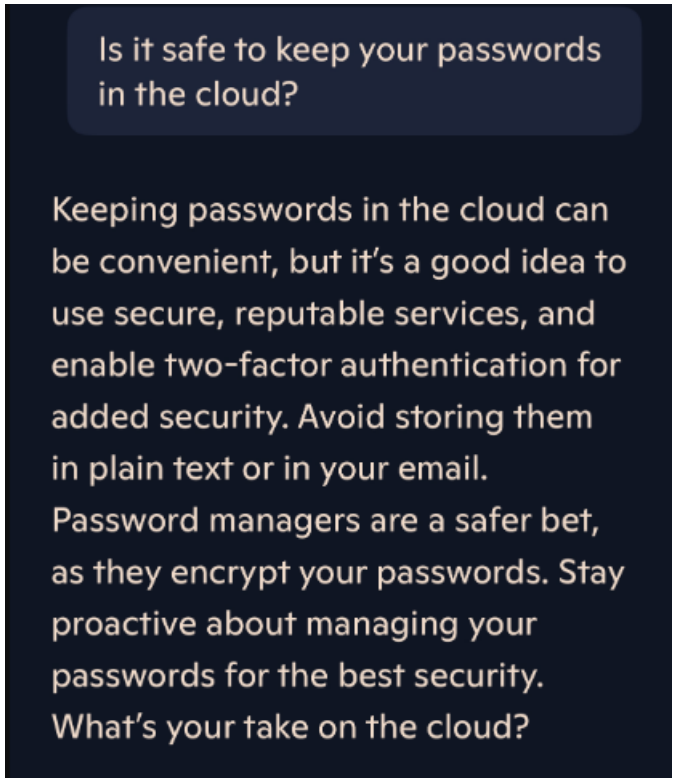
1. **1Password**: Known for its user-friendly interface and strong security features, it's a great choice for both beginners and advanced users [1].
2. **Bitwarden**: This is a fantastic free option that covers all the basics without costing anything [1]. It also has a premium plan for additional features [1].
3. **NordPass**: Offers a sleek design and comprehensive security features, including data breach reports and secure sharing options [2].



4. **Dashlane**: Great for its password health tool and customizable password options [2].
5. **Keeper**: Known for its robust security and multifactor authentication options [3].

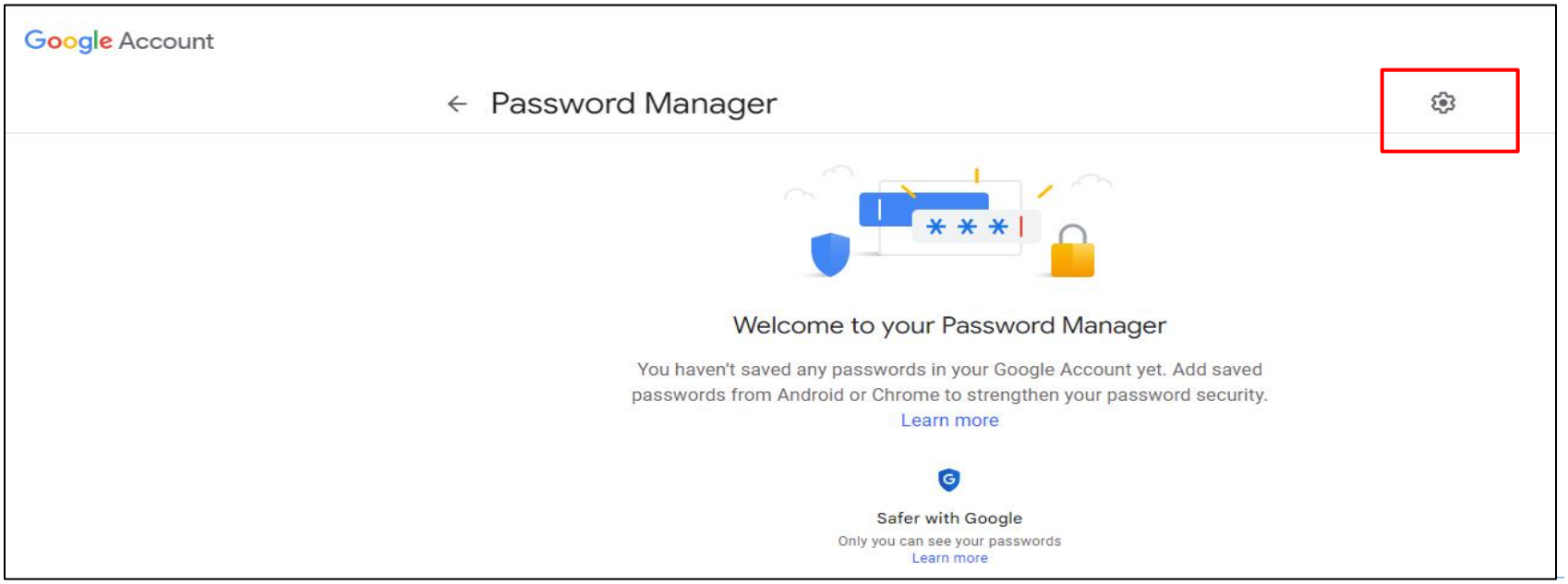
Each of these has its own unique features, so it might be worth considering what's most important to you, such as cost, ease of use, or specific security features. Do any of these stand out to you?

AI on Passwords in the Cloud

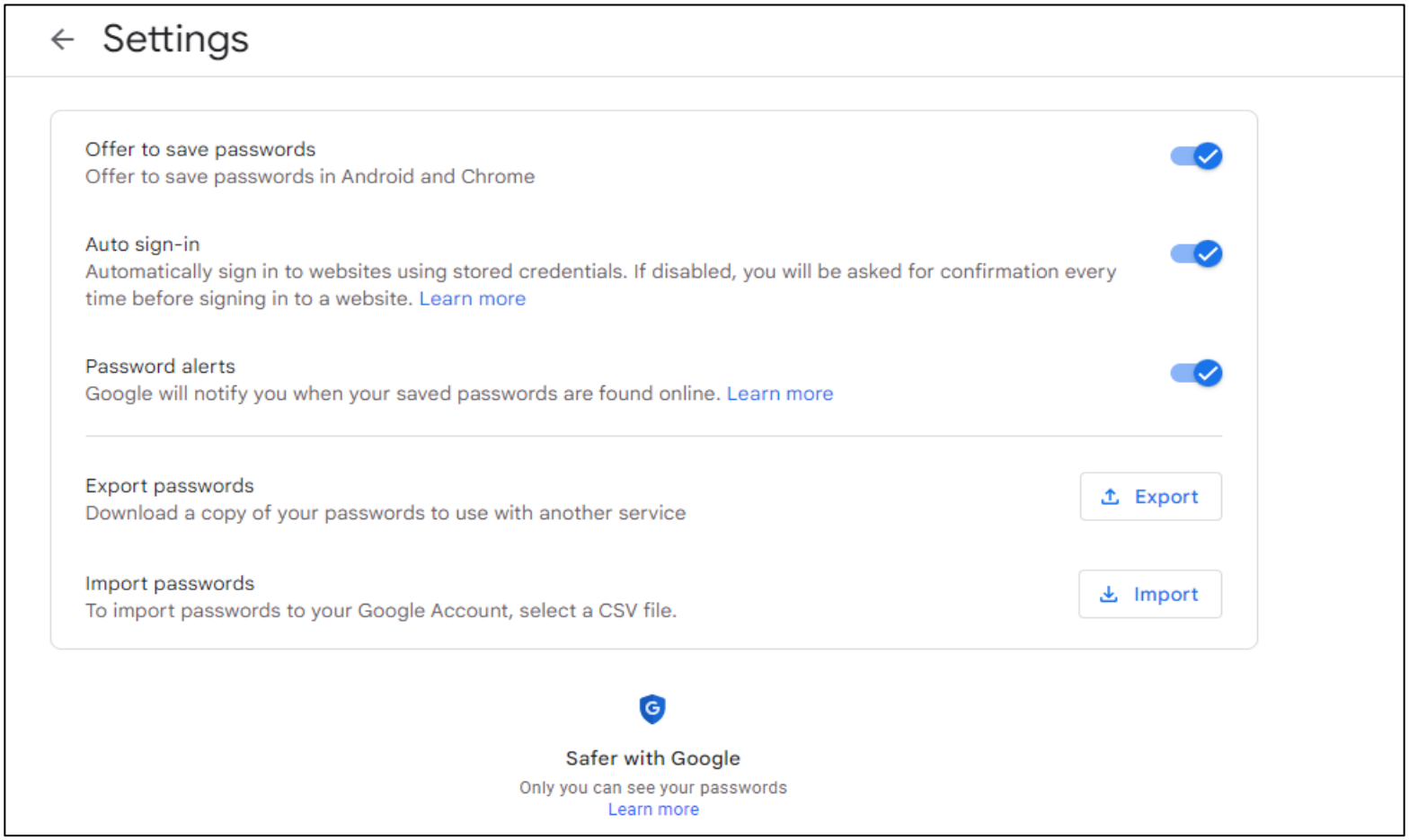


Google Chrome – Managing Passwords

- Log into your Google Account
- Click Account Icon (upper right corner)
- Click Manage Your Google Account
- Search Passwords
- Select Password Manager - Click Settings Icon

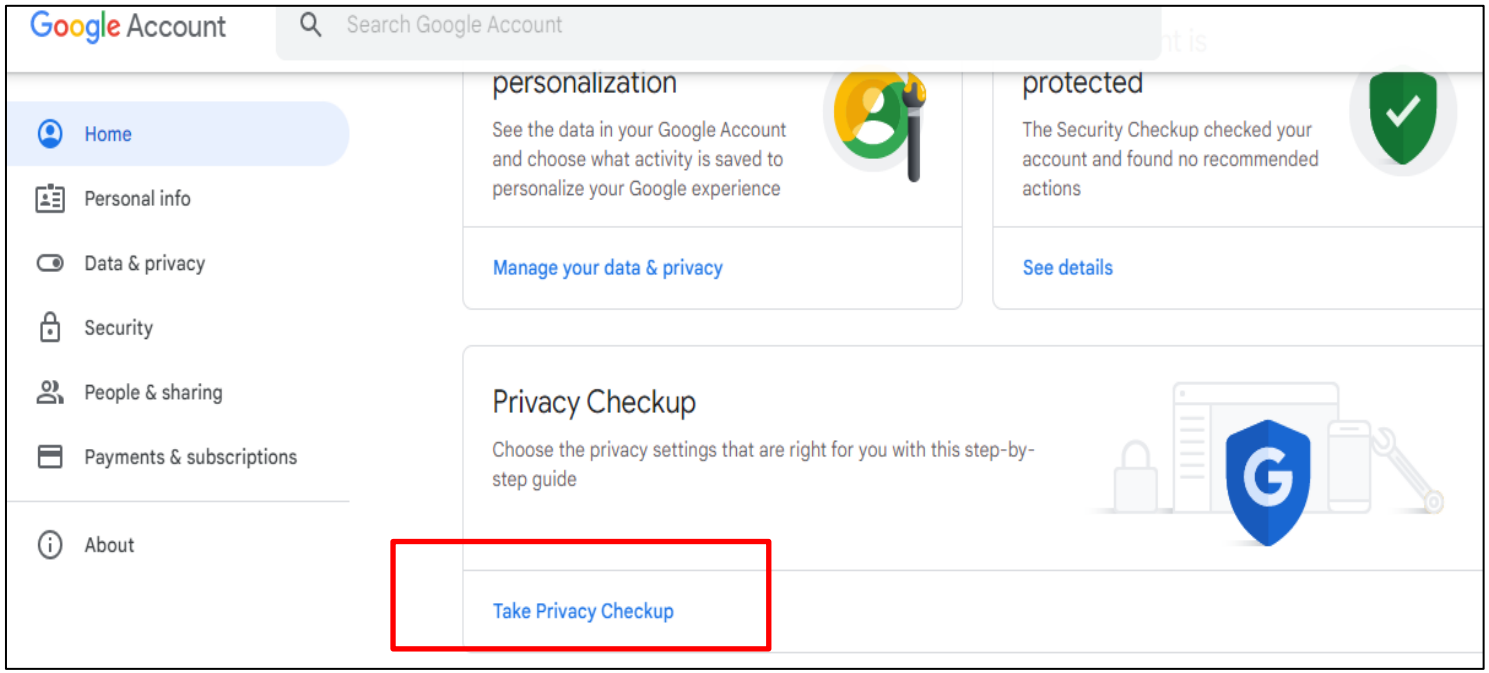


Google Password Manager - Settings

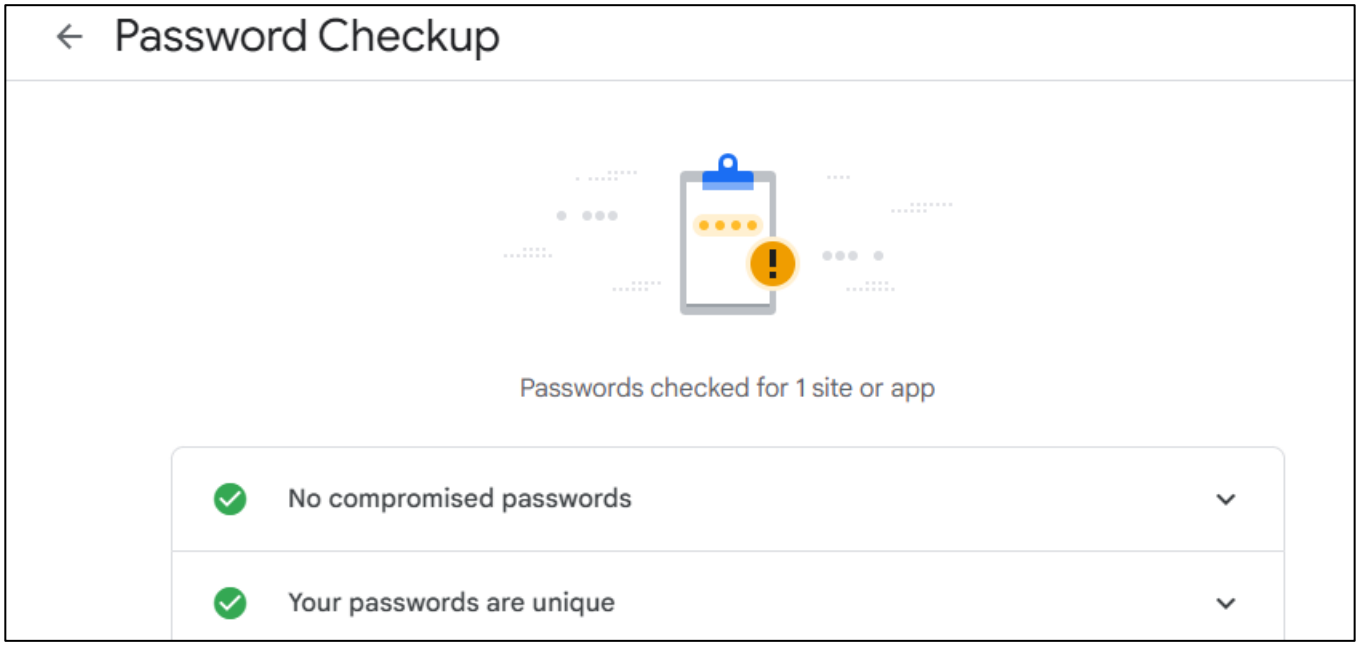


Google Account – Password Checkup

- Log into your Google Account
- Click Manage Your Account
- Click Take Privacy Checkup

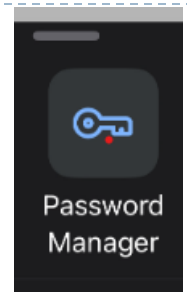


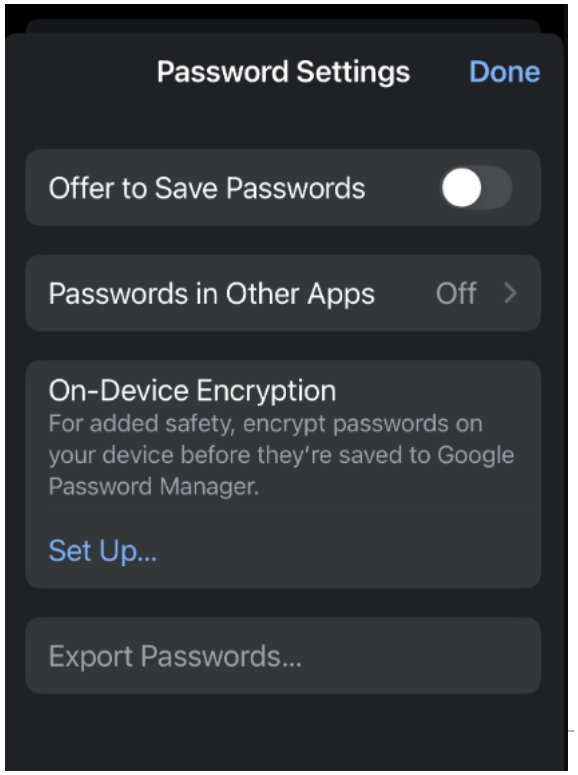
Google Account – Password Checkup

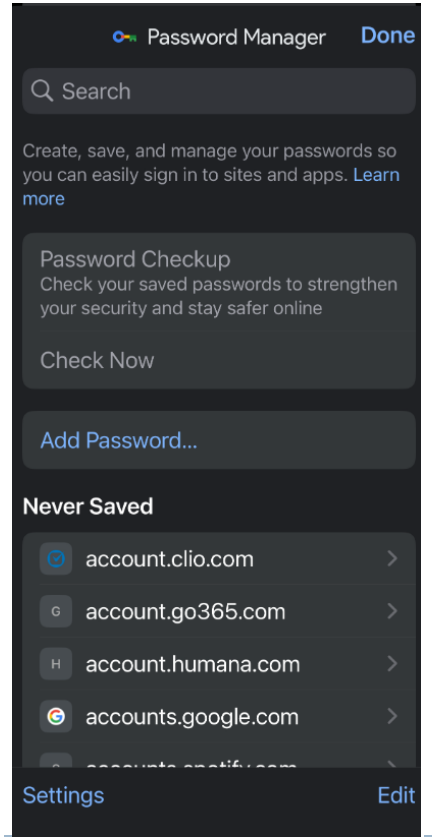


Google Chrome – iPhone

- Access Google Chrome on your iPhone
- Click … below.
- Click Password Manager







Digital Legacy

Digital Legacy – What Not to Do

- Best Plan – Create a List
  - Computers & Smart Devices
  - Internet Service Providers
  - Email Accounts
  - Photo Storage Sites
  - Social Networking – Facebook, Twitter, etc.
  - Online Subscriptions
  - Financial Sites
- Naming a Digital Executor
  - Trust at least one person with your online security information
  - Should have access to your computer files and online accounts – logins, passwords and instructions

Digital Legacy – What Not to Do

- Don’t put private info like usernames and passwords in your Will – Will Becomes a Public Document
- Leave Instructions with your Executor
- Facebook – Memorial Status
  - Memorialized Accounts – Place for friends and family to gather and share memories after a person has passed
  - The word “Remembering” will be shown next to the person’s name on their profile
- https://www.facebook.com/help/103897939701143/?ref=u2u
- Other Companies will delete or deactivate the account

Facebook – Deleting Account after Death

Deleting your account when you pass away

You can choose to have your account permanently deleted should you pass away. This means that when someone lets us know that you've passed away, all of your messages, photos, posts, comments, reactions and info will be immediately and permanently removed from Facebook. Your main profile and any additional Facebook profiles will also be deleted.

To request that your account be deleted:

1. From your main profile, click your profile photo in the top right of Facebook.
2. Select **Settings & Privacy**, then click **Settings**.
3. Below **General Profile Settings**, click **Memorialization Settings**.
4. Scroll down, click **Request that your account be deleted after you pass away** and click **Delete After Death**.

For friends and family

If you'd like to create another place for people on Facebook to share memories of your loved one, we suggest creating a group.

Learn how to request the memorialization of a profile or how to request the removal of a deceased person's profile from Facebook.

Computer & Laptop Guide

- If you do not pass on access to your computer or laptop before you pass there is a high probability that all the content saved on the device will remain inaccessible and never be retrieved.
- Passing on a password or granting access in advance might help safeguard the content. Content safeguarded may include personal photos, videos and documents.
- Granting access and safeguarding your content might further help to ensure that it remains accessible for your loved ones following your death and for generations to come.

Computer & Laptop Guide – Sharing Passwords

- ✓ Tell someone you trust the password for your computer / laptop (you might also want to do this for other password protected devices).
- ✓ Each time you update your password inform the person you trust what the new password is.
- ✓ If you do not want anyone to obtain access to your computer or laptop after you have died tell someone your wishes.

Mobile Phone Guide

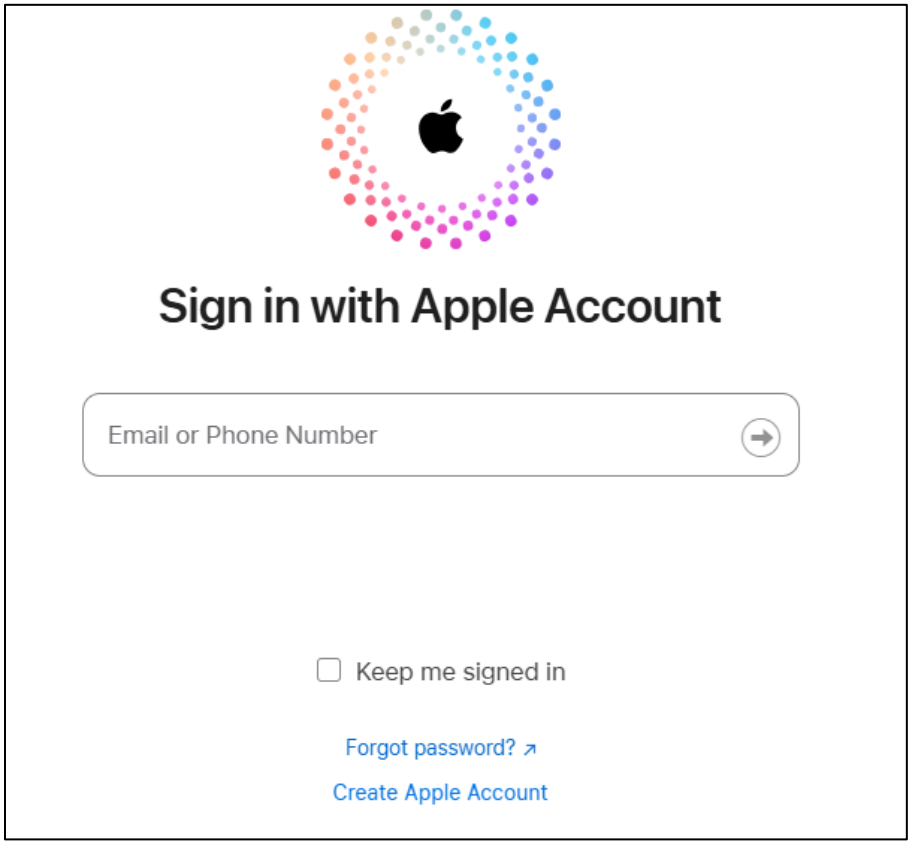
- Does someone other than yourself know the password for your mobile phone?
- Mobile phone manufacturers (like Apple and Samsung) do not provide any assistance to the recently bereaved when trying to access a mobile phone. This often is also the case regardless of whether or not directions were left in the deceased's 'last will & testament. (violates their privacy agreement with the deceased).

Mobile Phone Checklist

- ✓ Do you have a password / lock for your mobile phone? If so, have you told at least one person what it is?
- ✓ Have you transferred / backed up the photos and videos on your phone?
- ✓ Have you transferred / backed up the photos and videos on the phones that you have previously owned?
- ✓ Have you written down / told someone what you would like to happen to your mobile phone and the media on it once you have died?
- ✓ Would you or your next of kin like to keep your phone in order to view the messages you shared whilst alive?
- ✓ Is your mobile phone your main 'phonebook' and address list? If so, would you like your next of kin to have access to the contact list in order to arrange your funeral at a later date?

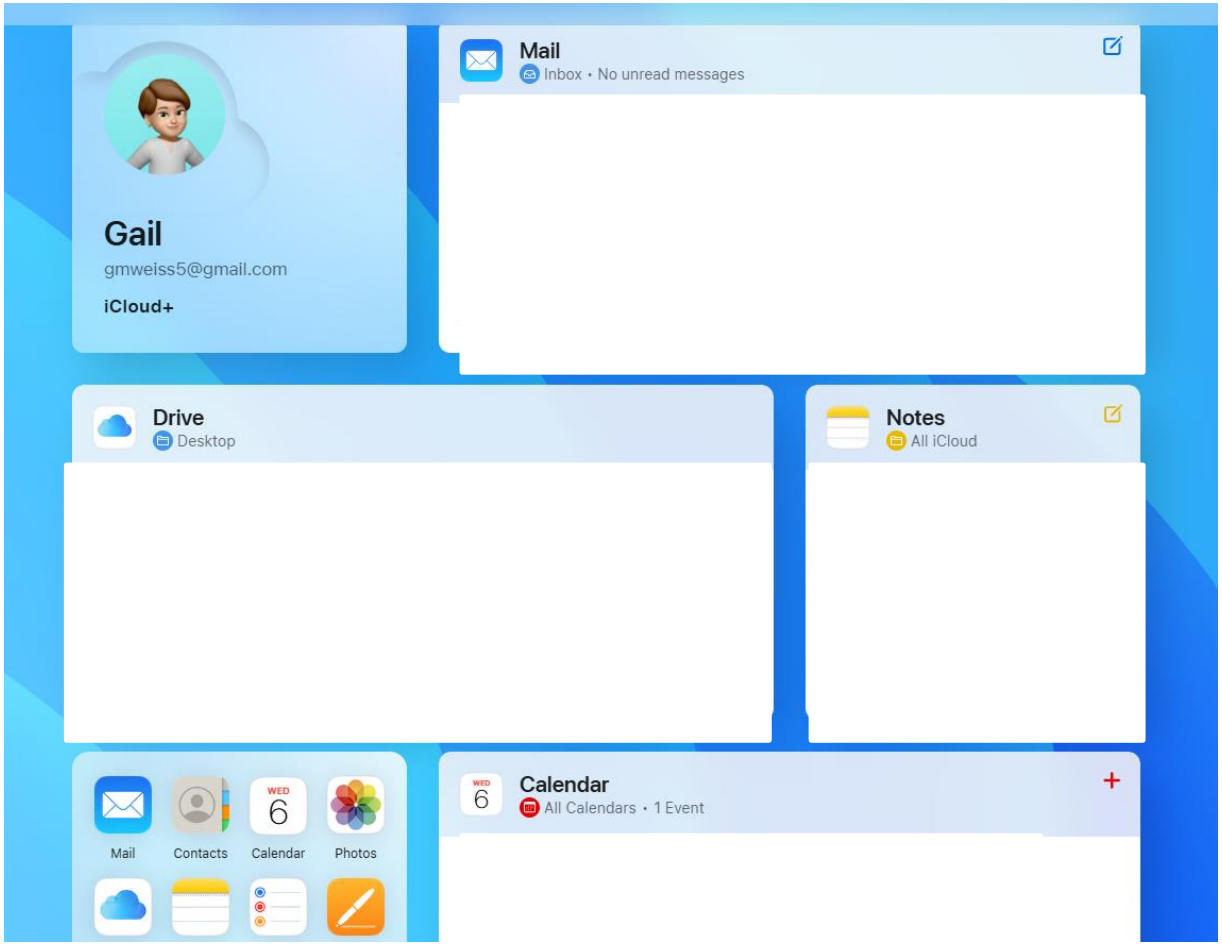
Access to your iCloud Account

- www.icloud.com



iCloud Account

- Contains all the data from your iPhone

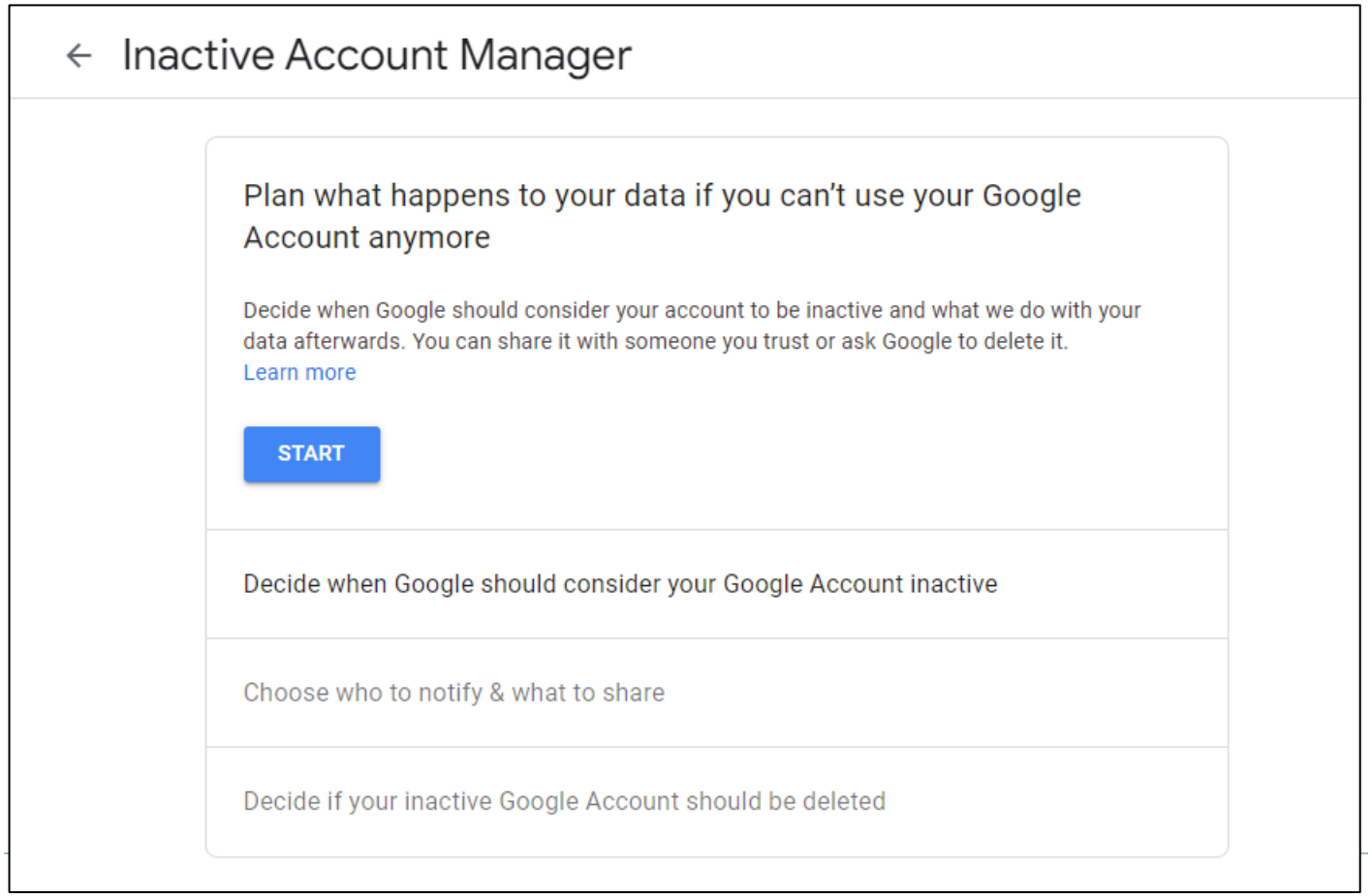


Google

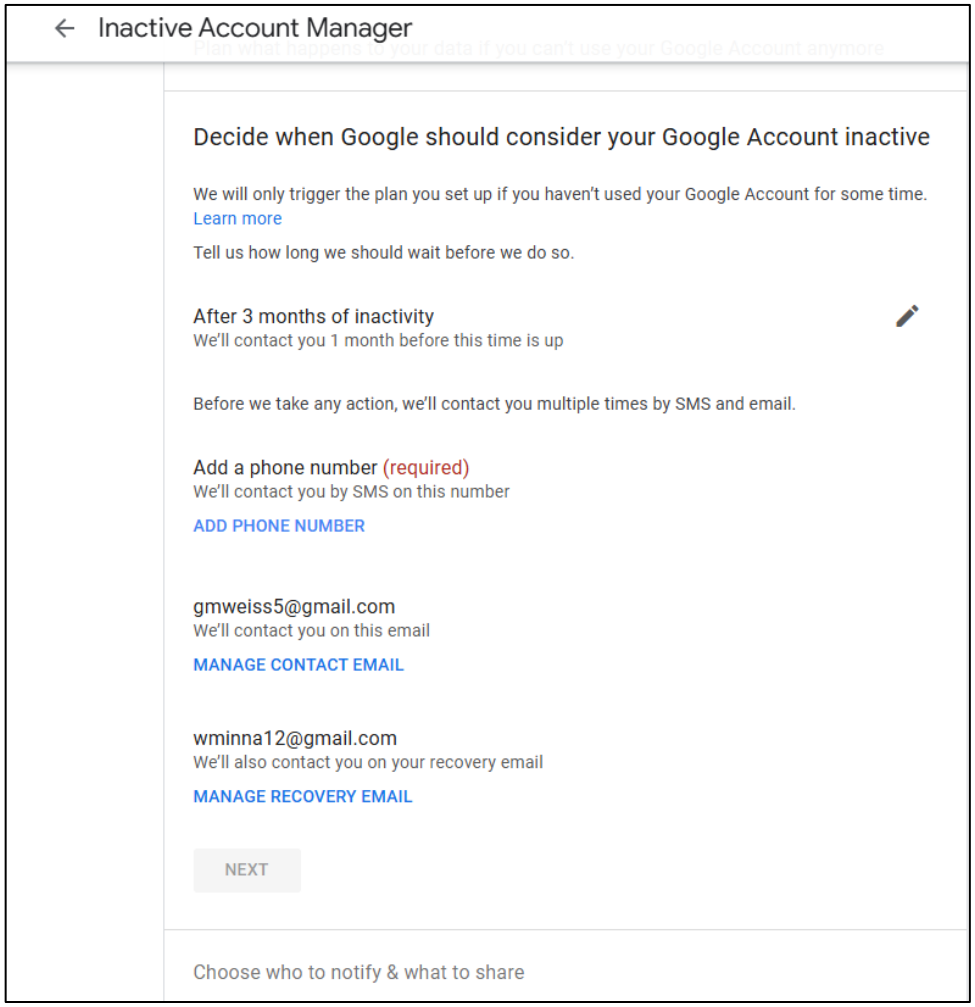
- If you have any of the following accounts: **Gmail (Googlemail) Google+, Google photos, Youtube etc** you can assign a digital executor to have access to some or all of the content saved on these services.
- To setup Google Inactive Account manager and assign your data saved with Google to you next of kin, use the Inactive Account Manager feature.

Google – Inactive Account Manager

- Manage Google Account
- Search for Inactive Account Manager



Google – Inactive Account Manager



Photos, Music & Other Files

- How will your Executor access the files and what you want done with the files after they have been accessed
- Eventually the account will be disabled, and no one will be able to access the files
- Make sure your Executor has the information he/she needs to access the account and download the files
- Leave these items to your loved ones in the will – “all my photographs of our trip… stored in my Google account”

Financial Accounts and Utilities

- Leave clear instructions for your Executor to access all your financial accounts and utilities online
- Use your will or trust to leave the contents of your financial accounts to your loved ones
- Your executor in the meantime will need access to these accounts to pay bills and wrap up your estate
- Make sure you have a document with clear instructions to the executor

List of Accounts & Passwords

- List – given to one of your heirs or in a safe deposit box – NOT in your file cabinet at home
- Password Manager – give Executor Master Password
- Excel Spreadsheet with Passwords – should give a copy to your executor or heir

Example of a Digital Legacy Template

The Digital Legacy Association - Social Media Will Template

Completing this template is a quick and simple way for you to list your online accounts and social media sites. Once it has been completed please PRINT it and keep it in a safe place.

Social Media Will Template for (Enter Your Name)			
Online Accounts / Social Media Sites	Username/ Email Address	How do you want this account to be managed (close, memorialize, deactivate)?	Have you downloaded a copy of your files on this account (support)

*Insert Extra cells when required

Links to More Info re: Digital Legacy

Digital Legacy Association

Device Guides	Social Media Guides
Computer and Laptop guide	Facebook guide
Mobile phone guide	
Tablet guide	
-	
	Google guide
	-
Further support and tutorials can be found:	www.DigitalLegacyAssociation.org